Committee on Ways and Means
Subcommittees on Oversight and Social Security
QFRs from May 8, 2012 hearing on Identity Theft and Tax Fraud

1. **How can the Internal Revenue Service (IRS), the U.S. Treasury Inspector General for Tax Administration (TIGTA), and other law enforcement work to catch criminals sooner? Are there additional tools that you need which would require legislative action?**

   Reducing identity theft-related tax fraud and detecting it sooner is a growing challenge. In many cases, the IRS and TIGTA are not aware that an identity theft-related fraudulent refund has been issued until the victim taxpayer notifies authorities or the criminals are caught trying to negotiate the fraudulent refunds. This can often be months or even years after the initial crime has occurred, making it even more difficult to address.

   No single law enforcement agency possesses the necessary resources to curtail, through classic criminal investigation and prosecution methods, the current increase in identity theft. TIGTA has a limited number of criminal investigators to cover our broad law enforcement jurisdiction and mission. We have directed our management team to coordinate with their counterparts in IRS Criminal Investigation to address identity theft-related tax fraud that falls within TIGTA's jurisdiction. TIGTA investigates identity theft when an IRS employee is involved in the scheme or uses their access to taxpayer identity information to commit the crime. TIGTA also has jurisdiction if a tax preparer steals client information in furtherance of an identity theft scheme or if an individual or group impersonates the IRS to carry out identity theft schemes.

   The best way to prevent the identity theft epidemic would be to ensure the IRS has the necessary information and time to better identify and stop the fraudulent refund before it is issued. Once a fraudulent refund is issued by the IRS, the prospects of recovering the erroneous refund are significantly diminished.

   In addition, the IRS can expand the use of information gathered from known identity theft cases to improve identity theft fraud screening tools. These tools are used to identify questionable tax returns for further review before tax refunds are issued.

   The IRS is currently working with the Department of Justice to pilot an approach in Florida of providing to local law enforcement, with the victim's consent, information from the return that was filed by the suspected identity thief. This would help local law enforcement identify those who may be part of a criminal enterprise involving identity theft-related tax fraud.

   Regarding possible legislative changes, the IRS can significantly improve the detection of false tax returns and the issuance of fraudulent tax refunds if it had

access to third-party income and withholding documents at the time tax returns were filed. Employers and other businesses are not required to file income and withholding documents until the end of February (end of March, if filed electronically), which is well after individuals start filing their tax returns.

As an alternative to the income and withholding documents, the IRS could benefit from expanded access to the Department of Health and Human Services' National Directory of New Hires (NDNH). Such access would enable the IRS to verify income for many individuals at the time tax returns are filed and before tax refunds are paid. The IRS has included a request for expanded access to the NDNH in its past annual budget submissions, including those for Fiscal Years 2010, 2011, and 2012. The request was made as part of the IRS's efforts to strengthen tax administration. However, expanded access has not been provided for in the law. The IRS has again included a request for expanded access to the NDNH as part of its Fiscal Year 2013 budget submission.

2. **Your testimony indicates that identity theft is growing and will be with us for the foreseeable future. Has this year been the largest year ever for attempts at tax fraud through identity theft? Do you see this trend continuing in the years ahead?**

   Yes, based on IRS statistics, it appears to be the largest year for attempts at tax fraud through identity theft. Since Calendar Year 2009, when the IRS began tracking identity theft incidents, the number of incidents of identity theft that the IRS identified has grown from about 366,000 in Calendar Year 2009 to over 1 million in Calendar Year 2011. Unfortunately, it does appear that the trend will continue for the foreseeable future.

   Additionally, using characteristics from tax returns the IRS identified and confirmed as filed by identity thieves, we identified approximately 1.5 million additional undetected Tax Year 2010 tax returns with potentially fraudulent tax refunds totaling in excess of $5.2 billion. Combined with the identity theft the IRS was able to detect, this indicates individuals used stolen identities to file approximately 2.4 million false tax returns and claimed $11.7 billion in potentially fraudulent tax refunds in Tax Year 2010.

3. **Your report indicates the only way to deal with this crime is to act offensively to thwart the criminal from the start. Once it gets to the IRS, chances are the criminal is going to be rewarded with a refund. Do you have any other suggestions for stopping ID theft related tax fraud, particularly like those thefts that occurred in Florida and Puerto Rico?**

   To effectively combat identity theft, several aspects need to be addressed: real-time access to income and withholding documents at the time tax returns are

filed, improving the IRS's ability to detect the fraudulent claims for refund prior to issuing tax refunds, continued collaborative law enforcement intervention that targets those cases that send the strongest deterrent message, and ensuring that the victim taxpayer's IRS tax accounts are timely resolved and corrected.

The IRS should also work with financial institutions to improve authentication controls for the direct deposits of tax refunds, including deposits to debit cards. In addition, the IRS needs to limit the number of tax refunds that can be deposited to one bank account or debit card and implement Treasury regulations requiring Federal tax deposits to be made only to accounts in the taxpayer's name.

The IRS implemented a number of initiatives during the 2012 Filing Season to improve the detection and prevention of fraudulent tax refunds from identity theft. These include new identity theft screening filters. The IRS also expanded the use of deceased taxpayer account locks and Identity Protection Personal Identification Numbers (IP PINs) to deter identity theft and prevent victims of identity theft from being victimized again. The IRS stated that it worked with the Social Security Administration to obtain records of Social Security benefits paid and the associated withholding earlier than in the past and is now using this information to verify tax returns as they are filed. The IRS has also initiated efforts to improve its ability to recover questionable tax refunds held by financial institutions. We have not yet audited these new initiatives, but plan to do so in the next fiscal year.

4. **Your report sates it can take the IRS more than one year to resolve an identity theft case. Is that a best-case scenario or is there a range?**

The time it takes to resolve identity theft cases is calculated using a range and is dependent on various factors, including the actual time an IRS assistor has to work a case to the time it takes the taxpayer to respond to IRS requests for information. The IRS does not have standards for how long it should take to work identity theft cases. Each function and office that works identity theft cases sets its own standards.

The IRS calculated that it took an average of 234 days to resolve identity theft cases involving duplicate tax returns in Calendar Year 2011. However, the system the IRS used to track and manage the majority of identity theft cases was implemented as an inventory control system, not to track and work the complex identity theft taxpayer correspondence cases. The IRS calculated the time from when it received the correspondences to the time when the case is closed. However, one taxpayer's case may be opened and closed multiple times as it changes case category codes (category codes denote the source of the case). This will skew the results.

Our review of a judgmental sample of 17 unique taxpayer cases classified as identity theft and originating in five functions showed:

- Case resolution averaged 414 days; cases were open from three to 917 days. Time was calculated from the date a taxpayer's case(s) was first opened until the last day when the case(s) closed.[1] This does not include the additional time after a case is closed for the taxpayers to receive any applicable tax refunds.
- Inactivity on cases averaged 86 days; inactivity ranged from 0 to 431 days.
- Concerning these 17 taxpayers, the IRS opened 58 different cases and assigned multiple assistors to work each case. The case histories did not state why the cases were reassigned. However, it appears that the cases were reassigned to manage inventory, i.e., reassigned to an assistor who had fewer cases in his or her inventory. Additionally, when the IRS received new documentation from the taxpayer or another IRS office, a new case was opened rather than the documentation correctly linked to the existing case. We made numerous recommendations, which should help the processes.

5. What can the IRS do to better assist victims and reduce the time to resolve their cases? What has the IRS done to address the problems identified by TIGTA and the Taxpayer Advocate?

In our May 2012 audit report,[2] we reported that communications between identity theft victims and the IRS were limited and confusing, and victims were asked multiple times to substantiate their identity. We recommended that the IRS conduct an analysis of the letters sent to taxpayers regarding identity theft and ensure that taxpayers are notified when the IRS has received their identifying documents.

Most identity theft cases involving individual duplicate tax returns are worked by the IRS's Accounts Management function. IRS employees who work in the Accounts Management function are assistors, who also spend hours working the telephones responding to taxpayer requests as well as working paper cases. However, Accounts Management function assistors are not examiners and are not trained to conduct examinations. We recommended that the IRS create a specialized unit in the Accounts Management function to exclusively work identity theft cases.

In August 2011, the IRS issued the *Identity Theft Program Future State Report*,[3] which provides its vision for the future state of the Identity Theft Program. It plans to reorganize to have an Identity Theft Program Specialized Group within each of the business units and/or functions, strengthen roles and responsibilities of the office responsible for the Identity Theft Program, and begin collecting IRS-wide

[1] Some taxpayers had multiple cases open involving more than one tax year.
[2] TIGTA, Ref. No 2011-40-050, *Most Taxpayers Whose Identities Have Been Stolen Do Not Receive Quality Customer Service* (May 2012).
[3] IRS, *IRS Identity Theft Program Future State Report* (Aug. 2011).

identity theft data to assist in tracking and reporting the effect of identity theft on tax administration. The IRS has begun revising guidelines and providing training for employees who interact with identity theft victims and work identity theft cases. In Fiscal Year 2012, the IRS plans to begin collecting IRS-wide identity theft data to be used to oversee the Identity Theft Program and issue a report to stakeholders.

The IRS also took a number of steps in the 2012 Filing Season to detect identity theft tax refund fraud before it occurs. These efforts included designing new identity theft screening filters that the IRS indicates will improve its ability to identify false tax returns before those tax returns are processed and prior to issuance of a fraudulent tax refund. As of April 19, 2012, the IRS had stopped the issuance of approximately $1.3 billion in potentially fraudulent tax refunds as a result of the new identity theft filters.

In addition, the IRS expanded efforts to place identity theft indicators on taxpayer accounts to track and manage identity theft incidents. For example, at the initiation of the 2012 Filing Season, the IRS and the U.S. Department of Justice announced the results of a massive nationwide crack down on suspected identity theft perpetrators as part of stepped-up efforts to combat tax refund fraud. This national effort is part of a comprehensive identity theft strategy by the IRS that is focused on preventing, detecting, and resolving identity theft cases as quickly as possible.

The IRS expanded its efforts to prevent the payment of fraudulent tax refunds claimed using deceased individuals' names and Social Security Numbers. Similar to last filing season, the IRS placed a unique identity theft indicator on deceased individuals' tax accounts. The indicator alerts the IRS when a tax return is filed using the deceased individual's Social Security Number. According to the IRS, as of March 31, 2012, the IRS placed a deceased lock on more than 164,000 tax accounts and has prevented approximately $1.8 million in fraudulent tax refunds claimed using deceased individuals' identities since the lock was established.

Once identity thieves successfully use an identity to obtain a fraudulent tax refund, they often attempt to reuse the identity in subsequent years to continue to file fraudulent tax returns. To prevent recurring identity theft, the IRS places an identity theft indicator on each tax account for which it has determined an identity theft has occurred. All tax returns filed using the identity of a confirmed victim of identity theft are flagged during tax return processing and sent for additional screening before any tax refund is issued. This screening is designed to detect tax returns filed by identity thieves who attempt to reuse a victim's identity in subsequent years and to prevent the issuance of fraudulent tax refunds.

Finally, the IRS is issuing the IP PIN to selected victims of identity theft. The IP PIN tells the IRS that the tax return was filed by the legitimate taxpayer and bypasses additional screening for identity theft, thus reducing delays in issuing the tax refund. The IRS issued an IP PIN to 251,568 individuals for the 2012 Filing Season and plans to issue an IP PIN to all taxpayers with identity theft indicators on their accounts for the 2013 Filing Season.

6. Are the victims notified?

The IRS notifies some victims of identity theft. The IRS has processes in place to detect multiple filings of tax returns using the same Social Security Number. When the IRS detects a tax return that uses a Social Security Number that has already been used to file a tax return, it notifies the taxpayer that the Social Security Number has already been used. The IRS then begins research to determine which tax return is the valid filing. However, the IRS does not tell the taxpayer that he or she may be the victim of identity theft.

Instead, when the taxpayer's tax return is rejected, the taxpayer is asked to complete Form 14039, *Identity Theft Affidavit*, and mail it with a paper tax return to the IRS. Once the IRS receives the paper tax return, a technician enters the data into the IRS's computer system, and forwards the tax return and affidavit to assistors who determine if it is an identity theft case and attempt to resolve it.

However, many identities that are used for tax refund fraud involve those individuals who do not have a tax return filing requirement. Since these individuals do not file a tax return, the IRS may only receive the false tax return filed by the identity thief and may not realize that the legitimate taxpayer's identity has been stolen. In these situations, the legitimate taxpayers may never know that they have been victims of tax-refund-fraud identity theft.

7. Should State and local law enforcement have access to taxpayer information, such as refund data, in pursuing identity theft cases? Why or why not?

An identity theft victim may consent to the disclosure of the false return filed by the alleged identity thief to State and local law enforcement agencies. As mentioned above, the IRS is currently piloting an approach in Florida of providing to local law enforcement, with the victim's consent, information from the return that was filed by the suspected identity thief.

Whether State and local law enforcement should have expanded access to information without the consent of the identity theft victim, or access to other investigative information currently protected by the confidentiality provisions of the Internal Revenue Code, is a question of tax policy and, pursuant to Treasury Order 111-01, should be posed to the Department of the Treasury's Office of Tax Policy.

8. **Can you comment on the content of the returns that are resulting in fraudulent refunds through identity theft? Are these individuals claiming that they paid more taxes than were due, or are they generally claiming refundable tax credits, such as the Earned Income Tax Credit and Additional Child Tax Credit?**

   The common characteristic of the approximately 1.5 million confirmed identity theft cases and the additional tax returns TIGTA identified is that false income and sufficient withholding were reported on the tax return to generate a refund. Without the false income, many of the deductions and/or credits used to inflate the fraudulent tax refund could not be claimed on the tax return.

   The top credit claimed was the Making Work Pay Credit (73 percent of the identity theft cases). Most of the returns involving tax fraud refund identity theft identified for Tax Year 2010 received this credit. After the Making Work Pay Credit, 36 percent claimed the Earned Income Tax Credit, and 20 percent claimed the Additional Child Tax Credit. A small percentage (less than 1 percent) claimed the First-Time Homebuyer's Credit.

   Direct deposit, which now includes debit cards,[4] is often used by identity thieves to obtain fraudulent tax refunds. Of the 1.5 million confirmed identity theft tax returns, 1.2 million (82 percent) used direct deposit to obtain potentially fraudulent tax refunds totaling approximately $4.5 billion, according to an upcoming TIGTA audit report.

9. **Law enforcement and Federal prosecutors make decisions on what cases to pursue based on competing priorities and varying levels of fraud. People hear of the $130 million cases being pursued, but how much of this problem exists at lower levels - $5,000 in fraud or $20,000 in fraud – and are these cases vigorously pursued? Do prosecutors only get interested when fraud reaches the incredible levels we read about in newspapers?**

   The Department of Justice has established general criteria for Federal prosecutions. The criteria are largely based upon the Department of Justice annual prosecution priorities along with each United States Attorney's Office's available resources.

   The substantial growth in this form of crime has quickly outstripped available resources. Based on such limitations, the role of Federal law enforcement is to select those cases that will have a broad impact on the criminal activity and that will send a strong deterrent message. The Department of Justice is also challenged with ensuring that they bring significant prosecutions throughout their spectrum of prosecution priorities and consistent with their available resources.

[4] These include prepaid debit cards as well as reloadable cards.

In addition, there do not appear to be any significant proposed increases in future budget years for additional investigative or attorney resources to address the challenges of the increasing identity theft criminal activity.

Questions from Congressman Tom Reed:

10. I have submitted an article from a Florida newspaper for the record that reports that most fraudulent IRS refunds are made on prepaid debit cards. I am concerned that the government is moving to the debit card payments system, not only for tax refunds, but all government payments before adequate measures to prevent fraud are in place. Are you aware of any analysis or studies that were available to Treasury or completed by Treasury outlining the hazards versus the benefits of debit card and electronic payments rather than paper checks?

We contacted the Department of the Treasury for its response to this question. Its response is as follows:

There are documented instances of fraudulent enrollments resulting from various identify theft scams where the perpetrator obtains sufficient information about the legitimate beneficiary. Similar fraud has occurred with other prepaid card providers and affiliated financial institutions.

As widely reported in the media, fraudsters use various techniques including lottery scams to obtain banking and other personal information needed to make unauthorized changes to direct deposit enrollments. Identify theft can also occur when a paper check is stolen from a recipient's mailbox.

Statistics show that electronic payments remain substantially safer than paper checks and are part of the reason why the Treasury Department has been promoting Direct Deposit for over 30 years and is currently moving to an all-electronic environment. In FY 2011, Treasury issued approximately 106 million Social Security and Supplemental Security Income checks. Of those checks, 440,000 or .0042% were reported lost or stolen and had to be replaced. As a comparison, that same year, Treasury issued over 661 million Social Security and Supplemental Security Income direct deposit payments, including many to prepaid cards. For example, the 4,007 fraud cases reported for Treasury's Direct Express program represent a tiny fraction of all direct deposit payments and the over 18 million Direct Express deposits made last year. Additionally, this past year, $70 million worth of Treasury-issued checks were fraudulently endorsed vs. the approximate $1.8 million reported with the Direct Express fraud cases (of which $900,000 has already been recovered). The reported fraud cases associated with the electronic payments

represent a tiny fraction when compared to those associated with the significantly lower volume of checks.[5]

11. What plans did Treasury have ready to address the crime of identity theft when they promulgated their regulation?

We contacted the Department of the Treasury for its response to this question. Its response is as follows:

Treasury is working closely with Comerica Bank (Treasury's financial agent for Direct Express) and SSA on efforts related to fraud detection, the monitoring of phishing scams, and other mitigating actions to reduce the occurrence of fraudulent enrollments. This includes suspending website enrollment functionality, flagging suspicious accounts, implementing more stringent processes for authenticating individuals enrolling and changing addresses and shifting enrollments to alternate channels with more stringent authentication.[6]

12. In your testimony, you recommend Treasury establish policies ensuring that only those institutions that can authenticate the identities of the card users be permitted in the debit card program for purposes of tax refunds. Can you expand on your suggestion? Should that same policy be used for payment of government benefits? Do you have other suggestions for protecting payment of benefits from identity theft?

We believe a policy which addresses both authenticating the identity of the card user and ensuring that the tax refund is deposited to an account only in the name of the individual is needed. Such a policy would help ensure that the Federal Government can identify and verify that the correct taxpayer will receive the tax refund. A broader policy for all government benefits would have the same effect; however, it is beyond the scope of our authority to make such a recommendation for all government benefits.

In a September 2008 report, we found that the IRS was not in compliance with direct deposit regulations that require tax refunds to be deposited to an account only in the name of the individual listed on the tax return.[7] The IRS still has not developed sufficient processes to ensure tax refunds are deposited to an account in the name of the filer. We recommended that the Department of the Treasury coordinate with responsible Federal agencies and banking institutions to develop a process to ensure that tax refunds issued via direct deposit to either a bank

---

[5] U.S. Department of the Treasury, Office of Financial Access, Financial Education, and Consumer Protection.
[6] Ibid.
[7] TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (Sept. 2008).

account or a debit card account are made only to an account in the taxpayer's name.

There continues to be a problem with a substantial number of refunds going to a single account, which increases the likelihood that the deposits are fraudulent. From the cases we identified with characteristics of identity theft, we identified 10 bank accounts that each had over 300 questionable Tax Year 2010 tax refunds deposited by the IRS. We have previously recommended, and continue to recommend, that the IRS limit the number of tax refunds issued via direct deposit to the same bank account or debit card account in an attempt to reduce the potential for fraud.

13. **Last year, the Treasury Department conducted a pilot program where low-income Americans could choose to receive their tax refund on a debit card instead of a check. I understand the report on this pilot program was sent to Treasury in late 2011, but has not yet been released publically. When can we expect a copy of the report?**

Department of the Treasury officials advised us that they are preparing the report to be released and shared with Congress in July 2012.